CLAIMS

What is Claimed is:

1. A system for controlling access to digital services comprising:

(a) a control center configured to coordinate and provide digital services;

(b) an uplink center configured to receive the digital services from the control center and transmit the digital services to a satellite;

(c) the satellite configured to:

(i) receive the digital services from the uplink center;

(ii) process the digital services; and

(iii) transmit the digital services and configuration information for accessing the digital services to a subscriber receiver station;

(d) the subscriber receiver station configured to:

(i) receive the digital services and configuration information from the satellite;

(ii) control access to the digital services through an integrated receiver/decoder (IRD);

(e) a conditional access module (CAM) communicatively coupled to the (IRD), wherein the CAM is configured to receive the configuration information, and wherein the configuration information has been transmitted asynchronously; and

(f) a custom logic block within the CAM, wherein the custom logic block is configured to dynamically reconfigure a hardware state machine in the CAM based on the configuration information, wherein the hardware state machine comprises custom logic that is used to control access to the digital services.

2. The system of claim 1 wherein the CAM comprises a smart card.

3. The system of claim 1 wherein the configuration information is encrypted.

4. The system of claim 3 wherein the configuration information is encrypted through a key exchange protocol.

5. The system of claim 4 wherein the key exchange protocol comprises a public key algorithm.

6. The system of claim 3 wherein the configuration information is received in uniquely encrypted, group encrypted packets.

7. The system of claim 3 wherein the custom logic block is further configured to:

decrypt the configuration information; and

store the configuration information in one or more protected registers.

8. The system of claim 1 wherein the custom logic block is further configured to verify that the configuration information is authentic.

9. The system of claim 8 wherein the custom logic block is further configured to retain the configuration information if the configuration information is authentic.

10. The system of claim 1 wherein the custom logic block is further configured to receive a synchronous command to reconfigure the hardware state machine using the configuration information.

11. The system of claim 1 wherein the hardware state machine is not directly accessible to a system input/output module or system bus of the security component.

12. The system of claim 1 wherein the custom logic block comprises an asynchronous dynamic pre-permutation module that employs a series of one or more configurable multiplexors at the beginning of the hardware state machine.

13. The system of claim 1 wherein the custom logic block comprises an asynchronous dynamic post-permutation module that employs a series of one or more configurable multiplexors at the end of the hardware state machine.

14. The system of claim 1 wherein the custom logic block comprises a dedicated hardware reconfiguration and input/output module that connects the hardware state machine to a system bus of the CAM and controls access to logic of the hardware state machine.

15. A method for providing access to digital services comprising:

(a) receiving configuration information in a security component, wherein:

(1) the configuration information has been transmitted asynchronously; and

(2) the security component is configured to control access to the digital services; and

(b) dynamically reconfiguring a hardware state machine in the security component based on the configuration information, wherein the hardware state machine comprises custom logic that is used to control access to the digital services.

16. The method of claim 15 wherein the security component comprises a smart card.

17. The method of claim 15 wherein the configuration information is received through a broadcast stream, Internet, callback, or other distribution channel.

18. The method of claim 15 wherein the configuration information is encrypted.

19. The method of claim 18 wherein the configuration information is encrypted through a key exchange protocol.

20. The method of claim 19 wherein the key exchange protocol comprises a public key algorithm.

21. The method of claim 18 wherein the configuration information is received in uniquely encrypted, group encrypted packets.

22. The method of claim 18 further comprising:

decrypting the configuration information; and

storing the configuration information in one or more protected registers.

23. The method of claim 15 further comprising verifying the configuration information is authentic.

24. The method of claim 23 further comprising retaining the configuration information if the configuration information is authentic.

25. The method of claim 15 further comprising receiving a synchronous command to reconfigure the hardware state machine using the configuration information.

26. The method of claim 15 wherein a component of the hardware state machine is not directly accessible to a system input/output module or system bus of the security component.

27. The method of claim 15 wherein the dynamic reconfiguration of the hardware state machine reconfigures a permutation that employs a series of one or more configurable multiplexors at the beginning of the hardware state machine.

28. The method of claim 15 wherein the dynamic reconfiguration of the hardware state machine reconfigures a permutation that employs a series of one or more configurable multiplexors at the end of the hardware state machine.

29. The method of claim 15 wherein a dedicated hardware reconfiguration and input/output module connects the hardware state machine to a system bus of the security component and controls access to logic of the hardware state machine.

30. A system for providing access to digital services comprising:

(a) a conditional access module (CAM) configured to receive configuration information for accessing the digital services, wherein the configuration information has been transmitted asynchronously; and

(b) a custom logic block configured to dynamically reconfigure a hardware state machine in the CAM based on the configuration information, wherein the hardware state machine comprises custom logic that is used to control access to the digital services.

31. The system of claim 30 wherein the CAM comprises a smart card.

32. The system of claim 30 wherein the configuration information is received through a broadcast stream, Internet, callback, or other distribution channel.

33. The system of claim 30 wherein the configuration information is encrypted.

34. The system of claim 33 wherein the configuration information is encrypted through a key exchange protocol.

35. The system of claim 34 wherein the key exchange protocol comprises a public key algorithm.

36. The system of claim 33 wherein the configuration information is received in uniquely encrypted, group encrypted packets.

37. The system of claim 33 wherein the custom logic block is further configured to:

decrypt the configuration information; and

store the configuration information in one or more protected registers.

38. The system of claim 30 wherein the custom logic block is further configured to verify that the configuration information is authentic.

39. The system of claim 38 wherein the custom logic block is further configured to retain the configuration information if the configuration information is authentic.

40. The system of claim 30 wherein the custom logic block is further configured to receive a synchronous command to reconfigure the hardware state machine using the configuration information.

41. The system of claim 30 wherein the hardware state machine is not directly accessible to a system input/output module or system bus of the CAM.

42. The system of claim 30 wherein the custom logic block comprises an asynchronous dynamic pre-permutation module that employs a series of one or more configurable multiplexors at the beginning of the hardware state machine.

43. The system of claim 30 wherein the custom logic block comprises an asynchronous dynamic post-permutation module that employs a series of one or more configurable multiplexors at the end of the hardware state machine.

44. The system of claim 30 wherein the custom logic block comprises a dedicated hardware reconfiguration and input/output module that connects the hardware state machine to a system bus of the CAM and controls access to logic of the hardware state machine.

45. An article of manufacture for providing access to digital services comprising:

(a) means for receiving configuration information in a security component, wherein:

(1) the configuration information has been transmitted asynchronously; and

(2) the security component is configured to control access to the digital services; and

(b) means for dynamically reconfiguring a hardware state machine in the security component based on the configuration information, wherein the hardware state machine comprises custom logic that is used to control access to the digital services.

46. The article of manufacture of claim 45 wherein the security component comprises a smart card.

47. The article of manufacture of claim 45 wherein the configuration information is received through a broadcast stream, Internet, callback, or other distribution channel.

48. The article of manufacture of claim 45 wherein the configuration information is encrypted.

49. The article of manufacture of claim 48 wherein the configuration information is encrypted through a key exchange protocol.

50. The article of manufacture of claim 49 wherein the key exchange protocol comprises a public key algorithm.

51. The article of manufacture of claim 48 wherein the configuration information is received in uniquely encrypted, group encrypted packets.

52. The article of manufacture of claim 48 further comprising:

means for decrypting the configuration information; and

means for storing the configuration information in one or more protected registers.

53. The article of manufacture of claim 45 further comprising means for verifying the configuration information is authentic.

54. The article of manufacture of claim 53 further comprising means for retaining the configuration information if the configuration information is authentic.

55. The article of manufacture of claim 45 further comprising means for receiving a synchronous command to reconfigure the hardware state machine using the configuration information.

56. The article of manufacture of claim 45 wherein a component of the hardware state machine is not directly accessible to a system input/output module or system bus of the security component.

57. The article of manufacture of claim 45 wherein the dynamic reconfiguration of the hardware state machine reconfigures a permutation that employs a series of one or more configurable multiplexors at the beginning of the hardware state machine.

58. The article of manufacture of claim 45 wherein the dynamic reconfiguration of the hardware state machine reconfigures a permutation that employs a series of one or more configurable multiplexors at the end of the hardware state machine.

59. The article of manufacture of claim 45 wherein a dedicated hardware reconfiguration and input/output module connects the hardware state machine to a system bus of the security component and controls access to logic of the hardware state machine.